

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-23623

(P2002-23623A)

(43) 公開日 平成14年1月23日 (2002.1.23)

(51) Int.Cl.⁷

G 0 9 C 1/00

識別記号

6 1 0

F I

G 0 9 C 1/00

テ-リ-ト* (参考)

6 1 0 B 5 J 1 0 4

審査請求 未請求 請求項の数9 OL (全 14 頁)

(21) 出願番号 特願2000-212175(P2000-212175)

(22) 出願日 平成12年7月13日 (2000.7.13)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 村谷 博文

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

(72) 発明者 佐野 文彦

東京都府中市東芝町1番地 株式会社東芝

府中事業所内

(74) 代理人 100083161

弁理士 外川 英明

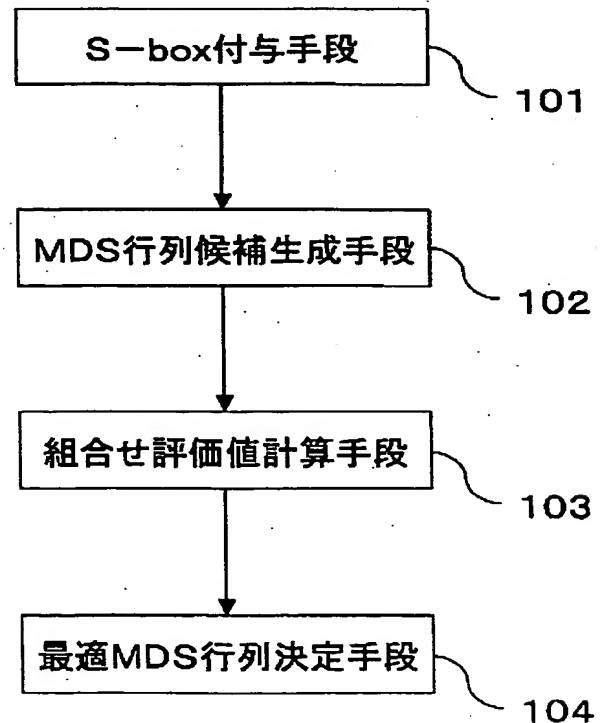
最終頁に続く

(54) 【発明の名称】 パラメータ決定装置、パラメータ決定方法、暗号化装置、および復号装置

(57) 【要約】

【課題】 S-boxとMDS行列を構成要素を含む暗号化装置において、S-boxとMDS行列が、それぞれ、独立な設計方針により最適な複雑さを実現しようとしているにもかかわらず、相互に効果を相殺するで、かえってより安全ではない暗号化装置となってしまう恐れがあった。

【解決手段】 MDS行列要素の各候補に対して、ある与えられたS-boxに行列要素の乗算を行った結果の複雑さを評価し、この複雑さの評価結果に基づき、MDS行列を構成する行列要素候補の組合せに対する複雑さの評価を与え、また、このMDS行列に対する逆行列に対しても同様の複雑さの評価を与え、これらの行列に対する複雑さの評価結果に基づき、そのS-boxとの組合せにおいて、最適の複雑さを与えるMDS行列を決定する方法と、その方法によって得られたMDS行列を採用した暗号化装置を与える。



【特許請求の範囲】

【請求項1】 第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、該拡散処理の前記第2パラメータを決定するためのパラメータ決定装置であって、
該換字処理に用いられる決定済みの第1パラメータを入力する入力手段と、
該拡散処理に用いられる第2パラメータ候補を逐次生成する第2パラメータ候補生成手段と、
該入力手段によって入力された第1パラメータと、該第2パラメータ候補生成手段によって逐次生成される各第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算する計算手段と、
前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補を前記装置の第2パラメータと決定する最適パラメータ決定手段とを備えたことを特徴とするパラメータ決定装置。

【請求項2】 第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、該換字処理の前記第1パラメータを決定するためのパラメータ決定装置であって、
該換字処理に用いられる第1パラメータ候補を逐次生成する第1パラメータ候補生成手段と、
該拡散処理に用いられる決定済みの第2パラメータを入力する入力手段と、
該第1パラメータ候補生成手段によって逐次生成される各第1パラメータ候補と、該入力手段によって入力された第2パラメータとに基づいて、所定の方法によって評価値を逐次計算する計算手段と、
前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第1パラメータ候補を前記装置の第1パラメータと決定する最適パラメータ決定手段とを備えたことを特徴とするパラメータ決定装置。

【請求項3】 第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、該換字処理の前記第1パラメータを決定するためのパラメータ決定装置であって、
該換字処理に用いられる第1パラメータ候補を逐次生成する第1パラメータ候補生成手段と、
該拡散処理に用いられる第2パラメータ候補を逐次生成する第2パラメータ候補生成手段と、
該第1パラメータ候補生成手段によって逐次生成される第1パラメータ候補と、
該第2パラメータ候補生成手段によって該拡散処理部行列候補生成手段によって逐次生成される第2パラメータ

候補とに基づいて、所定の方法によって評価値を逐次計算する計算手段と、
前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第1パラメータ候補および第2パラメータ候補をそれぞれ前記装置の第1パラメータおよび第2パラメータと決定する最適パラメータ決定手段とを備えたことを特徴とするパラメータ決定装置。

【請求項4】 行列により平文の各文字間を置換する拡散処理を行う装置の、該拡散処理の前記行列を決定するために前記行列に最適な共通因子を決定するパラメータ決定装置であって、
該拡散処理に用いられる決定済みの行列を入力する入力手段と、
該拡散処理の行列に対し、括り出し可能な共通因子の候補を生成する共通因子候補生成手段と、
該共通因子候補生成手段によって逐次生成される共通因子候補によって該拡散処理の行列を括り出した後の行列に基づいて、所定の方法によって評価値を逐次計算する計算手段と、
該計算手段によって計算された評価値から最適な評価値を決定し、この決定した評価値に対応する共通因子候補を共通因子とする最適共通因子決定手段とを備えたことを特徴とするパラメータ決定装置。

【請求項5】 第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、パラメータ決定方法であって、該換字処理と該拡散処理との組み合わせによって定まる所定の方法にて計算された評価値が最適にするように第1パラメータあるいは第2パラメータあるいはそれら両方のパラメータを決定することを特徴とするパラメータ決定方法。

【請求項6】 第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、行列により平文の各文字間を置換する拡散処理とを行う装置の、該拡散処理の前記行列を決定するためのパラメータ決定装置であって、
該換字処理に用いられる決定済みの第1パラメータを入力する入力手段と、
該拡散処理に用いられる行列の一要素である第2パラメータ候補を逐次生成する第2パラメータ候補生成手段と、
該入力手段によって入力された第1パラメータと、該第2パラメータ候補生成手段によって逐次生成される各第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算する計算手段と、
前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補を前記行列の一要素の第2パラメータと決定する最適パラメータ決定手段とを備え、

前記行列の全ての要素を決定することを特徴とするパラメータ決定装置。

【請求項7】 前記最適パラメータ決定手段は、更に、得られた評価値から所定数の適した評価値を決定し、この決定した評価値に対応する第2パラメータ候補を前記行列の他の要素のパラメータ候補とすることを特徴とする請求項6のパラメータ決定装置。

【請求項8】 平文を暗号化するために、平文の各文字を別のものに変換する複数の換字処理部と、平文の各文字間を置換する拡散処理部とを備える暗号化装置であって、

前記拡散処理部は、

該換字処理部に用いられる決定済みの第1パラメータと、逐次生成される該拡散処理に用いられる第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算して得られた評価値の中から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補を平文の各文字間の置換のために用いられるようにしたことを特徴とする暗号化装置。

【請求項9】 暗号文を復号するために、暗号文の各文字を別のものに変換する複数の換字処理部と、暗号文の各文字間を置換する拡散処理部とを備える復号装置であって、

前記拡散処理部は、該換字処理部に用いられる決定済みの第1パラメータと、逐次生成される該拡散処理に用いられる第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算して得られた評価値の中から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補を平文の各文字間の置換のために用いられるようにしたことを特徴とする復号装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、秘匿のためにデジタルデータを暗号化する暗号化装置、及び、必要に応じて復号するために用いる復号装置に関する。

【従来の技術】

【0002】 暗号系には、メッセージの暗号化と復号において同じ鍵を用いる秘密鍵暗号系と暗号化と復号で異なる鍵を用いる公開鍵暗号系がある。最も良く知られている秘密鍵暗号は、DES (Data Encryption Standard) と呼ばれる米国標準ブロック暗号である。暗号解読は、平文（暗号化前のメッセージ）と暗号文（暗号化後のメッセージ）の対の集合から暗号化に用いられた鍵を求めることである。暗号解読には、平文がもともと持っていた冗長性 (redundancy) が利用されることが多い。

【0003】 Claude Elwood Shannon は、“Communication Theory of Secrecy Systems” (Bell System Technical Journal

1、28巻4号、1949年、656-715) という論文の中で、平文（暗号化前のメッセージ）が持っている冗長性を見えにくくする技法を、confusion と diffusion の2つの基本的な技法に分類した。

【0004】 confusion とは、平文と暗号文の間の関係を見えにくくすることで、暗号文の冗長性や統計的パターンを観測することで解読を行うことを難しくする。例としては、平文のアルファベットの各文字を暗号文のアルファベットの各文字に対応付ける換字表を鍵として1字1字変換する方法、換字 (substitution)、がある。diffusion とは、平文の冗長性を暗号文全体に広げることである。例としては、平文の文字の順序を置き換える転置 (transposition) がある。

【0005】 先ほど述べたDESにおいても、暗号化処理は、S-box と呼ばれる confusion の処理と P-box と呼ばれる diffusion 処理を基本的な処理として含んでいる。

【0006】 近年、DESの後継暗号として、AES (Advanced Encryption Standard) と呼ばれる次世代の米国標準ブロック暗号の仕様策定の作業が進められている。そこに提案された暗号は、DES以降の蓄積された暗号解読法の知見を反映して、confusion と diffusion にも新しい考え方が持ち込まれている。

【0007】 例えば、diffusion の働きをする設計上の構成要素としては、線形変換の層が採用されることが多い。しかも、できるだけ効率良く拡散を行ため MDS (Maximal Distance Separable) 符号を利用した線形変換層が提案されている。(Vincent Rijmen、Joan Daemen、“The Cipher SHARK”、Fast Software Encryption、LNCS 1039、99-112、1996。)

【0008】 このMDS符号を利用した線形変換層は、活性S-box数の下限を保証する性質があるため、その事実を利用して、差分解読法と線形解読法に関する強度を証明することができるという特長がある。

【0009】 差分解読法と線形解読法以外の主な解読法に対する対策は、換字層において行われており、線形変換層に対する新たな制約とはならない。

【0010】 例えば、差分解読法、線形解読法、高階差分解読法、補間攻撃法に対して安全となるよう、S-boxを有限体上のベキ関数やその和として設計する方法が提案されている。(盛合志帆、「差分／線形／高階差分／補間攻撃に対して強いS-boxの一構成法」、1998年暗号と情報セキュリティシンポジウム、2、2、C、1998年。)

【0011】 また、補間攻撃に対して安全にするため、

有限体上のベキ関数と剰余類環上のアフィン変換によってS-boxを構成する方法が提案されている。(M. Kanda et al., "E2-A New 128-Bit Block Cipher", IEICE Trans. Fundamentals., E83-A, 1, 48-58, 2000.)

【0012】つまり、現在の暗号設計の流儀では、差分解読法と線形解読法に対する対策としては、S-boxの適切な選択とMDS符号を利用した線形変換層の採用が行われるものの、差分解読法や線形解読法以外の解読法に対する対策としては、主として、S-boxの適切な選択によってのみ行われており、MDS符号としてどのようなものを採用すべきか積極的な選択指針が与えられていない。

【0013】MDS符号を利用した線形変換層を行列として表現した場合、それをMDS行列と呼ぶことにする。MDS行列の行列要素を決定する主な設計方針として、現在までに提案されているものの例は、AES候補であるRijndael暗号における設計方針としては、MDS行列をテーブルルックアップで実装する場合のテーブルサイズを小さくすること、MDS行列の行列演算を8ビットプロセッサで処理する場合に効率的に処理できること、がある。また、同じくAES候補であるTwofish暗号における設計方針としては、MDS行列の直後で用いられているPHT (Pseudo-Hadamard Transformation) との関係から、MDS行列が折角保証しているブランチ数をその直後のPHTが小さくしてしまう確率を小さくするよう行列要素を決定している。

【0014】つまり、従来、MDS行列の行列要素の選択基準は、処理効率や実装コストの観点によるものが主である。例外は、PHTなど、他の特殊なプリミティブとの関連から差分解読法や線形解読法に対する安全性を極力下げないようにするというものであった。Rijndael暗号の設計方針が言うように、8ビットプロセッサ上では、行列演算をテーブルルックアップではなく、プロセッサの算術演算や論理演算によって実装するため、タイミング攻撃に結びつく恐れもちろんあるため、行列要素を慎重に選択する必要があるという主張もあるのだが、特殊なプラットフォームに限定された問題と言える。

【0015】従来のように、S-boxとMDS行列を別々の設計方針で設計すると、S-boxが折角安全性を高めるための設計をされているにもかかわらず、MDS行列がその効果を相殺するような設計になってしまう恐れがある。

【0016】例えば、S-boxを出来るだけ複雑な関数として実現することで安全性を高めようとする場合を考える。例えば、 n ビットの入出力を持つS-boxの場合、入出力を $GF(2^n)$ の元とみなし、S-box

を $GF(2^n)$ から $GF(2^n)$ への関数とすると、その表現が単純な関数、具体的には、項数の少ない多項式や、分子の多項式の項数と分母の多項式の項数の和が小さい有理式、であるときには、補間攻撃が有効であることが知られている。(盛合志帆、下山武司、金子敏信、「SNAKE暗号の補間攻撃」、1998年暗号と情報セキュリティシンポジウム、7. 2. C、1998年。) 補間攻撃とは暗号化関数を未知の係数を持つ多項式や有理式で表現し、平文-暗号文の対を複数与えることで、これらの係数をラグランジュの補間法などによって決定する解読法である。

【0017】補間攻撃を避けるために、S-boxを構成する際に、単純なベキ乗関数だけでなく、 $GF(2^n)$ の代数構造に合わない処理、例えば、ビットの置換や別の代数構造における演算を利用する場合がある。この場合、S-boxは、複数のベキ乗関数による多項式として表現しなおすことができる。つまり、 $GF(2^n)$ の代数構造とは異質な演算を組み合わせることで、実質的に、多項式の項数を増やした効果を得ている。

【0018】この場合、S-boxに続くMDS行列が、その入力表現として、S-boxの出力の $GF(2^n)$ の表現と同じ表現を採用する場合には、MDS行列の行列要素が乗算される影響は、S-boxを表現しているベキ乗関数の多項式の各項に対して、定数の乗算を行うに過ぎないので、S-boxで項数を増やした効果を相殺するものとはならない。

【0019】ところが、MDS行列の入力の表現が、S-boxの出力の $GF(2^n)$ の表現とは異なる場合、例えば、ビット位置の役割が両表現で異なる場合や、MDS行列の入力において意図的にビット置換が行われる場合などがそうであるが、この場合、折角S-boxにおいて項数を増やすために行われた異質な演算の組合せの効果が、MDS行列の演算において相殺されてしまう可能性がある。

【0020】つまり、上の説明は、従来のように、S-boxとMDS行列が、それぞれ、別個の設計方針で、独立に補間攻撃への対策を採ってしまうと、逆に、それらが相殺する恐れがあることを指摘するものである。

【0021】次に、関数の複雑さを表す別の指標として、S-boxの出力ビットを入力ビットの論理式で表した場合の項数も考えられる。この指標は、厳密な証明を与えることは難しいが、我々は、アバランシュ性の目安になると考える。

【0022】アバランシュ性とは、入力に変化した場合に、その影響が出力の一部ではなく、できるだけ、広く影響する性質のことである。ビットの論理表現による項数が多ければ、出力ビットは、入力ビットに関して規則的な構造や、単純な表現となっていないと期待されるので、入力ビットの変化は、出力ビットに多様な変化をも

たらずことで高いアバランシュ性を実現できるのではないかと期待される。

【0023】この場合においても、S-boxとMDS行列が、それぞれ独立に、ビットの論理表現を複雑にするよう設計された場合に、その効果が相殺する場合がある。

【発明が解決しようとする課題】本発明は、S-boxとMDS行列が別々の設計方針で設計されるために、折角S-boxがある評価値で見たとき、安全性を高める設計をされているにも関わらず、MDS行列がその効果を相殺するような設計になってしまうという課題があった。

【0024】本発明は、このような問題点に鑑みてなされたものであり、暗号化装置または復号装置に適用する際に換字処理および拡散処理をできるパラメータ決定装置、パラメータ決定方法、暗号化装置、および復号装置を提供することを目的とする。

【課題を解決するための手段】上記目的を達成するために、本発明の請求項1のパラメータ決定装置は、第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、該拡散処理の前記第2パラメータを決定するためのパラメータ決定装置であって、該換字処理に用いられる決定済みの第1パラメータを入力する入力手段と、該拡散処理に用いられる第2パラメータ候補を逐次生成する第2パラメータ候補生成手段と、該入力手段によって入力された第1パラメータと、該第2パラメータ候補生成手段によって逐次生成される各第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算する計算手段と、前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補を前記装置の第2パラメータと決定する最適パラメータ決定手段とを備えた。

【0025】また、本発明の請求項2のパラメータ決定装置は、第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、該換字処理の前記第1パラメータを決定するためのパラメータ決定装置であって、該換字処理に用いられる第1パラメータ候補を逐次生成する第1パラメータ候補生成手段と、該拡散処理に用いられる決定済みの第2パラメータを入力する入力手段と、該第1パラメータ候補生成手段によって逐次生成される各第1パラメータ候補と、該入力手段によって入力された第2パラメータとに基づいて、所定の方法によって評価値を逐次計算する計算手段と、前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第1パラメータ候補を前記装置の第1パラメータと決定する最適パラメータ決定手段とを備えた。

【0026】また、本発明の請求項3のパラメータ決定装置は、第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、該換字処理の前記第1パラメータを決定するためのパラメータ決定装置であって、該換字処理に用いられる第1パラメータ候補を逐次生成する第1パラメータ候補生成手段と、該拡散処理に用いられる第2パラメータ候補を逐次生成する第2パラメータ候補生成手段と、該第1パラメータ候補生成手段によって逐次生成される第1パラメータ候補と、該第2パラメータ候補生成手段によって該拡散処理部行列候補生成手段によって逐次生成される第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算する計算手段と、前記計算手段によって逐次計算され、得られた評価値から最適な評価値を決定し、この決定した評価値に対応する第1パラメータ候補および第2パラメータ候補をそれぞれ前記装置の第1パラメータおよび第2パラメータと決定する最適パラメータ決定手段とを備えた。また、本発明の請求項4のパラメータ決定装置は、行列により平文の各文字間を置換する拡散処理を行う装置の、該拡散処理の前記行列を決定するために前記行列に最適な共通因子を決定するパラメータ決定装置であって、該拡散処理に用いられる決定済みの行列を入力する入力手段と、該拡散処理の行列に対し、括り出し可能な共通因子の候補を生成する共通因子候補生成手段と、該共通因子候補生成手段によって逐次生成される共通因子候補によって該拡散処理の行列を括り出した後の行列に基づいて、所定の方法によって評価値を逐次計算する計算手段と、該計算手段によって計算された評価値から最適な評価値を決定し、この決定した評価値に対応する共通因子候補を共通因子とする最適共通因子決定手段とを備えた。

【0027】本発明の請求項5のパラメータ決定方法は、第1パラメータにより平文の各文字を別の文字にそれぞれ変換する換字処理と、第2パラメータにより平文の各文字間を置換する拡散処理とを行う装置の、パラメータ決定方法であって、該換字処理と該拡散処理との組み合わせによって定まる所定の方法にて計算された評価値が最適にするように第1パラメータあるいは第2パラメータあるいはそれら両方のパラメータを決定するようにした。

【0028】また、請求項8の暗号化装置は、平文を暗号化するために、平文の各文字を別のものに変換する複数の換字処理部と、平文の各文字間を置換する拡散処理部とを備える暗号化装置であって、前記拡散処理部は、該換字処理部に用いられる決定済みの第1パラメータと、逐次生成される該拡散処理に用いられる第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算して得られた評価値の中から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補

を平文の各文字間の置換のために用いられるようにした。

【0029】また、請求項9の復号装置は、暗号文を復号するために、暗号文の各文字を別のものに変換する複数の換字処理部と、暗号文の各文字間を置換する拡散処理部とを備える復号装置であって、

【0030】前記拡散処理部は、該換字処理部に用いられる決定済みの第1パラメータと、逐次生成される該拡散処理に用いられる第2パラメータ候補とに基づいて、所定の方法によって評価値を逐次計算して得られた評価値の中から最適な評価値を決定し、この決定した評価値に対応する第2パラメータ候補を平文の各文字間の置換のために用いられるようにした。

【0031】これにより、暗号化装置または復号装置に適用する際に、性能の良い換字処理および拡散処理を有する暗号化装置および復号装置が提供できるようになった。

【発明の実施の形態】（第1実施形態）

【0032】以下、図面を参照しながら発明の実施の形態を説明する。本実施形態では、与えられたS-boxに対して、最適な組合せのMDS行列を決定する装置を示す。まず、本実施形態の基本的な構成例について説明する。

【0033】図1に、本発明の一実施形態に係る、与えられたS-boxに対して最適なMDS行列を決定する装置の構成を示す。

【0034】図1に示されるように、本最適MDS行列決定装置は、S-box付与手段(101)とMDS行列候補生成手段(102)と組合せ評価値計算手段(103)と最適MDS行列決定手段(104)とからなる。

【0035】図2は、本実施形態による装置が行う処理の流れを表している。

【0036】まず、S-box付与手段は、本決定装置以外の装置によって決定された、あるS-boxを指定する情報を受け入れる(201)。

【0037】S-boxは、一般には、mビット入力nビット出力の写像である。S-boxの記述は、どのような入力値に対してどのような出力値を持つかを示す表として記述することも可能であるし、関数として簡潔な表現が可能であるならば、関数の形で記述することも可能である。ここでは、いずれにせよ、S-boxを一意に特定できる情報が与えられるものとする。

【0038】次に、MDS行列候補生成手段は、当該付与されたS-boxと組み合わせるMDS行列の候補を、逐次、生成する(202)。次に、組合せ評価値計算手段は、当該付与されたS-boxと当該生成されたMDS行列候補の組合せの複雑度(評価値)を計算する(203)。次に、今計算したMDS行列候補が最後の候補であるか否かを判定する(204)。もし、まだ、

新たな候補が存在する場合には、201の処理に戻り、新たなMDS行列の候補を生成する。こうして、逐次生成された、複数のMDS行列候補に対して同様の処理を繰り返し、その各々に対して組合せの複雑度を求める。

【0039】ここで、組合せの複雑度とは、S-boxとMDS行列候補の組合せに対する複雑度の意味で、S-box単体、MDS行列単体の複雑度ではなく、その両者の組合せを一体として評価した場合の複雑度である。具体的に、評価値である複雑度の例としては、S-boxがnビット入出力の場合、S-boxの入出力をGF(2^n)の元として表現するとき、S-boxの入力で表現したMDS行列候補の出力の項数によって定義することができる。

【0040】別の複雑度の例としては、GF(2^n)の元としてではなく、ビット毎に晴らしてみた場合、S-boxの入力ビットによる論理式でMDS行列候補の出力ビットを表現した場合の項数をとる場合もある。204において、新たな候補が存在しない場合には、最後に、最適MDS行列決定手段は、こうして求めた、当該付与S-boxと当該生成された複数のMDS行列候補の各々の組合せの複雑度を元に、最適な組合せの複雑度を持つ組合せを決定し、そのMDS行列候補を最適なMDS行列として決定する(205)。この場合、評価値が複雑度である場合には、その値として項数が最大のものを選択する。

【0041】ここでは、評価値として項数を例に挙げたが、それ以外の評価値を用いても同様の処理によって最適なMDS行列を決定する装置を実現することは容易である。

【0042】図3は、より詳細に本実施形態の処理の流れを表す図である。まず、S-boxの入力が行われる(301)。この入力されたS-boxにおける出力を入力で表した多項式を求める(302)。次に、MDS行列の行列要素候補として取りうる値を生成する(303)。MDS行列の行列要素候補とは、MDS行列がGF(2^n)上の行列であれば、GF(2^n)の元を順々に生成すればよい。0は、GF(2^n)の元であるが、これを行列要素とすると行列はMDS行列にはなり得ないので、0を最初から除外して生成してもよい。

【0043】次に、S-boxの出力に、この行列要素候補を乗算した結果について、S-boxの出力を入力で表した多項式を求める(304)。この多項式に基づき、S-boxとこの行列要素候補の組合せに対する複雑度を計算する(305)。

【0044】複雑度としては、S-boxの入力やS-boxの出力と行列要素候補の乗算結果をGF(2^n)の元とみなして、S-boxの入力の多項式として表現された乗算結果の項数を用いる。この項数による複雑度の定義については、後で、図4および図5によって詳細に説明する。もちろん、項数による複雑度の定義は、複

雑度の一例であって、様々な理論的根拠や経験的ヒューリスティックスによって別の雑度の定義を用いても良い。例えば、多項式の次数にもとづいて雑度を定義しても良い。また、別の、雑度の例としては、有限体の元としてではなく、ビット単位で、出力ビットを入力ビットの多項式で表現した場合の項数によって雑度を定義しても良い。その際、項数は、すべての次数の項数を同じ重みで数えてもよいし、多項式に含まれる項の次数に応じて重み付きで数えても良い。さらには、最適化がどのような攻撃法に対する安全性を達成することを目的としているかによっては、雑度以外の評価値を定義しても良い。

【0045】次に、まだ別の行列要素候補が存在するか否かを判定する(306)。まだ、別の候補が存在する場合には、303の処理にもどり新たな候補を生成して同様の処理を繰り返す。別の候補が存在しない場合には、行列要素候補の中から必要な個数の候補を選択し、MDS行列候補を生成する(308)。

【0046】この際、全ての行列要素候補の組合せによってMDS行列候補を生成すると、非常に多くの組合せの数があるため、すべてのMDS行列候補に対する雑度の計算を行うことが非現実的となることがある。その場合には、305で計算した雑度に従って、雑度の大きないくつかの行列要素候補の集合の中から選ばれた行列要素候補によってMDS行列候補を生成することで、効率良く雑度の大きなMDS行列を探索することも可能である(307)。この場合、MDS行列候補の生成は、この絞り込まれた行列要素候補の中から行列要素を選択することによって生成される(308)。

【0047】次に、こうして生成されたMDS行列候補が、実際に、MDS行列となっているか否かを判定する(309)。この判定は、MDS行列候補に対して、そのすべての小行列式が非零であることを確認することによって行われる。行列候補がMDS行列とならない場合には、308の処理にもどり、次の行列候補を生成して同様の処理を繰り返す。行列候補がMDS行列となっている場合は、行列の雑度の計算を行う(310)。

【0048】行列の雑度は、306において求めたS-boxと行列要素候補の組合せに対する雑度を元に、MDS行列候補に属する行列要素候補の各々に対する雑度を足し合わせたものとして定義する。

【0049】次に、逆行列を求める(311)。そして、逆行列に対しても310と同様にS-boxと行列の組合せの雑度を求める(312)。

【0050】この場合、想定している暗号化処理や復号処理によっては、逆行列との組合せに用いるS-boxは、もとのS-boxの逆となるようにする変形例も可能である。

【0051】こうして求めた、MDS行列候補の雑度とその逆行列の雑度から、ともに、その雑度が大き

な候補を選択することで、最適なS-boxとMDS行列の組合せを決定する(313)。

【0052】上の例では、S-boxと逆行列の組合せに関する雑度まで評価したが、これを省略する変形例も可能である。その場合、311と312の処理は省略でき、313では、S-boxとMDS行列の組合せの雑度のみから最適な組合せを決定する。

【0053】図4は、S-boxと行列要素候補の組合せにおいて、出力を入力が多項式で表したときの雑度を説明する図である。S-boxの入出力が8ビットの場合の例である。401のS-boxへの入力ビットを i_0, i_1, \dots, i_7 で表す。402の行列要素候補をS-boxの出力に乗算した結果の出力ビットを o_0, o_1, \dots, o_7 と表す。入力と出力を有限体GF

(2^8)上の元と見なし、ベクトル表現によって、それぞれ、 $i = i_7 z^7 + i_6 z^6 + i_5 z^5 + i_4 z^4 + i_3 z^3 + i_2 z^2 + i_1 z + i_0$ 、 $o = o_7 z^7 + o_6 z^6 + o_5 z^5 + o_4 z^4 + o_3 z^3 + o_2 z^2 + o_1 z + o_0$ 、と表現する。ここで、 z は原始多項式 $x^8 + x^6 + x^5 + x + 1 = 0$ の根であるとする。評価値である雑度は、例えば、 o を i の多項式として表現した場合における多項式の項数として定義される。別の定義としては、 o を i の有理式として表現した場合における分子の多項式の項数と分母の多項式の項数の和として定義することも可能である。これらの雑度は、補間攻撃に対する耐性の目安となることが知られている。

【0054】また、雑度の別の定義としては、出力ビット、 o_0, o_1, \dots, o_7 、をビット毎に見て、それぞれ、入力ビット i_0, i_1, \dots, i_7 の論理式で表現した場合の項数をすべての出力ビットに関して和をとったものとして定義される。これは、この入出力間のアバランシュ性の目安となると思われる。また、間接的に、補間攻撃への耐性の目安にもあると思われる。

【0055】図5は、S-boxとMDS行列の組合せにおける雑度の説明をする図である。

【0056】501はS-box、502はMDS行列で表現された拡散層を表している。例えば、GF

(2^8)上のMDS行列の例で説明すると、その行列要素は、有限体GF(2^8)の元である。各S-boxの出力は、この拡散層を通過することによって、MDS行列の行列要素が乗算され、その結果を行方向に加算したものが拡散層の出力として現われる。この行列要素の乗算の部分だけを見ると、ちょうど、図4で説明した、S-boxと行列要素候補の組合せとなっていることがわかる。そこで、S-boxとMDS行列候補の組合せの雑度を、図4を用いて説明したS-boxと行列要素候補の組合せにおける雑度を元に、MDS行列候補の全ての行列要素に対して、この雑度の求め、その結果を足し合わせたものとして定義する。この定義を用いると、S-boxと行列要素候補の組合せの雑度が求ま

っていれば、S-boxとMDS行列候補の組合せに対する複雑度も求めることができる。

【0057】S-boxとMDS行列の組合せの複雑度に関するこの定義も、理論的根拠や経験的ヒューリスティックスによって異なる複雑度の定義を用いても良い。さらに、想定する攻撃法によっては、別の評価値の定義を用いて良い。

【0058】ここで述べた複雑度の定義は例であって、これら以外にも、想定する攻撃法に応じて、理論的根拠と経験的ヒューリスティックスに基づいた多様な複雑度や評価値を定義して用いる場合にも、本発明を適用できる。例えば、コストや速度や他の攻撃に対する安全性の目安となる量を採用したとしても、換字層(S-box)と拡散層(MDS行列)の組合せでもって、その評価値を最適化することによって、拡散層のパラメータを最適となるよう決定するという変形例も可能である。

【0059】図6は、以上に説明した装置によって、あるいは、別の方法や装置によって決定されたMDS行列による拡散層を極力小さな実装コストで実現したり、高速に動作するようにするために、MDS行列の一部を括りだす装置の構成を示している。図7は、この装置の処理の流れを表している。

【0060】ここで、括りだしとは、MDS行列の同一行や同一列の属する行列要素から共通の因子を取り出す処理のことである。例えば、GF(2⁸)上の4行4列MDS行列の第i列の行列要素が、a_{1i}、a_{2i}、a_{3i}、a_{4i}であるとする、これから共通因子a(ここで、aはGF(2⁸)の非零元とする。)を括りだすとは、これらの行列要素に対して共通因子aによる除算を行い、b_{1i}、b_{2i}、b_{3i}、b_{4i}とすることである。ここで、b_{1i}=a_{1i}/a、b_{2i}=a_{2i}/a、b_{3i}=a_{3i}/a、b_{4i}=a_{4i}/aである。このようにある列から共通因子を括り出すと行列が元の行列とは変わってしまうが、この共通因子aをMDS行列の直前に置かれたS-boxに対して繰り込むことで、S-boxと行列全体としてみると、括りだし前と後は同じ処理となっている。

【0061】ここで、因子aをS-boxに繰り込むとは、もともとのS-boxが入力xを出力y=f(x)に変換する写像であるとする、aを繰り込んだS-boxは入力xを出力y'=a×f(x)に変換する写像に変えることである。

【0062】括りだしによって実装コストが小さくなる理由について説明する。MDS行列のある列から括りだされた共通因子は、その列に入力しているS-boxに対応している。そこで、ある列から括りだされた共通因子を、そのS-boxに繰り込むことができる。S-boxはテーブルルックアップによって実現されることが多い。この場合、この共通因子の繰り込みは、テーブルの値を変更するだけで済むので、テーブルの大きさを変

えず、実装コストには影響しない。

【0063】一方、MDS行列は、一般に、テーブルサイズが大きくなるため、テーブルルックアップによって実現されるとは限らない。ハードウェアによる実装ならば結線によって、ソフトウェアならば命令の組合せによって実現することになる。この結線のコストや命令の組合せのコストは、共通因子括りだし後のMDS行列の行列要素の値に依存する。例えば、GF(2⁸)上の4行4列のMDS行列において、行列への入力をx₁、x₂、x₃、x₄、行列の出力をy₁、y₂、y₃、y₄、行列要素をa_{ij}とする。y_i=a_{i1}×x₁+a_{i2}×x₂+a_{i3}×x₃+a_{i4}×x₄である。例えば、a_{i1}が値として1を取るとき、a_{i1}×x₁の乗算は、x₁の各ビットの値がそのままa_{i1}×a₁の各ビットの値になるため、この乗算に相当するハードウェアはビット間の排他的論理和を行うための配線が不要である。同様にこの乗算に相当するソフトウェア命令の組合せもビット間の排他的論理和を行うためのビットシフト命令やマスク命令は不要である。つまり、a_{i1}が値1をとるときの実装コストは小さい。一般のa_{i1}の値ではa_{i1}×a₁は、ビット間の排他的論理和を行う必要があり、その必要な回数はa_{i1}の値によって異なる。したがって、実装コストは、行列要素の値によって異なる。このことから、共通因子の括りだしによって、実装コストの小さな行列要素からなるMDS行列への変換ができると、行列全体の実装コストは小さくて済む。

【0064】結線やソフトウェア命令の組合せによって実現する場合のコストに対する評価値として、ファンインを定義する。ファンインは、行列要素の乗算において、乗算後の各ビットが乗算前の何個のビットの排他的論理和で表現されているかを数え、その結果をすべての行列要素について足し合わせたものとする。ファンインは、MDS行列の行列要素の値によって決まるので、共通因子の括りだしによって、括りだし後の行列がファンインが小さな行列となっているならば、括りだした共通因子はS-boxに繰り込み、残された行列を実際に結線やソフトウェア命令の組合せによって実現することで実装コストを小さくすることができる。

【0065】図6が示すように、本装置は、MDS行列付与手段(601)と共通因子候補生成手段(602)とコスト評価値計算手段(603)と最適共通因子決定手段(604)とからなる。

【0066】図7は、このような最適な共通因子を見つけ出す装置の処理の流れを表している。まず、MDS行列付与手段によって、MDS行列が入力される(701)。次に、共通因子生成手段によって、括りだすべき共通因子の候補が生成される(702)。コスト評価値計算手段によって、この共通因子を括りだした後のMDS行列が計算される(703)。得られたMDS行列の

コスト評価値が計算される(704)。コスト評価値としては、例えば、先に述べたファンインがある。実装の方法によっては、別のコスト評価値を用いても良い。次に、括りだし後のMDS行列の逆行列を求める(705)。逆行列のコスト評価値を求める(706)。次に、まだ、別の共通因子の候補があるか判定する(707)。別の共通因子の候補がある場合には、702に戻り、新たな候補を生成し、以下同様の処理を行う。別の共通因子候補が無い場合には、最適共通因子決定手段が、それまでに求めたコスト評価値をもとに、最適な共通因子を決定する(708)。

【0067】図7の例では、共通因子をMDS行列で括りだし、その括りだしの結果から逆行列のコスト評価値を計算したが、MDS行列と逆行列でそれぞれ独立に共通因子のくくりだしを行うような変形も可能である。これは、暗号化の際のS-boxと復号の際のS-boxには、それぞれ、独立の共通因子を繰り込むことが可能であるからである。

【0068】また、共通因子は、MDS行列のすべての行列要素に共通の因子でも良いし、列毎あるいは行毎に異なる共通因子としても良い。

【0069】これまでは、MDS行列として最適なものを決定する装置の例を説明したが、図8は、MDS行列が与えられた場合に、それと最適な組合せのS-boxを決定する装置の構成を表している。図9は、その装置の処理の流れを表している。図10は、より詳細にその装置の処理の流れを説明している。

【0070】本装置は、MDS行列付与手段(801)とS-box候補生成手段(802)と組合せ評価値計算手段(803)と最適S-box決定手段(804)とからなる。

【0071】まず、MDS行列付与手段は、本決定装置以外の装置によって決定された、あるMDS行列を指定する情報を受け入れる(901)。次に、S-box候補生成手段は、当該付与されたMDS行列と組み合わせるS-box候補を、逐次、生成する(902)。次に、組合せ評価値計算手段は、当該付与されたMDS行列と当該生成されたS-box候補の組合せの複雑度(評価値)を計算する(903)。次に、今計算したS-box候補が最後の候補であるか否かを判定する(904)。もし、まだ、新たな候補が存在する場合には、901の処理に戻り、新たなS-box候補を生成する。こうして、逐次生成された、複数のS-box候補に対して同様の処理を繰り返し、その各々に対して組合せの複雑度を求める。もし、904において、新たな候補が存在しない場合には、最適S-box決定手段は、それまでに求めたMDS行列とS-box候補の組合せの複雑度をもとに、最適な組合せを決定する(905)。

【0072】より詳細に処理を説明する。まず、MDS

行列付与手段によって、MDS行列の入力が行われる(1001)。MDS行列は各行列要素の値を与えることで一意に特定できる。

【0073】次に、S-box候補生成手段によって、S-boxの候補の生成を行う(1002)。

【0074】ここで、S-box候補の生成方法の例としては、S-boxが入力値に対する出力値を表す表として記述できることより、相異なる値を持つ表を順次生成する方法がある。一般に、入出力のビット数が大きくなると、この方法で生成されるS-boxの総数は非常に多くなるため、すべての可能性を生成することは非現実的となる。そこで、別の生成方法の例としては、生成されるS-boxとして何らかの制約を課したものに限り方法がある。例えば、入力と出力をGF(2ⁿ)の元とみなしたとき、S-boxを入力xのべき乗関数x^kや異なるべきを持つべき乗関数の和 $\sum c_k \times x^k$ として表現できるものに限定して生成する方法も可能である。さらに、もう少し生成される個数を増やすならば、べき乗関数の和の前や後にビットの入れ替えを行ったものに制限して生成する方法も可能である。他には、アフィン変換などを組み合わせてもよい。

【0075】次に、組合せ評価値計算手段は、生成されたS-box候補における出力を入力で表した多項式を求める(1003)。次に、S-box候補とMDS行列の行列要素を乗算した結果について、S-box候補の入力による多項式を計算する(1004)。この多項式に基づき、S-box候補と与えられたMDS行列の組合せに対する複雑度を計算する(1005)。次に、MDS行列の逆行列を求める(1006)。

【0076】1006について、MDS行列が与えられた1001において、一度、逆行列を計算しておいて、あとで、その結果を繰り返し利用するような変形も可能である。

【0077】次に、S-box候補とこの逆行列に対して、多項式の計算を行う(1007)。次に、S-box候補と逆行列の組合せの複雑度を計算する(1008)。次に、まだ別のS-box候補が存在するか否かを判定する(1009)。まだ、別の候補が存在する場合には、1002の処理にもどり新たな候補を生成して同様の処理を繰り返す。別の候補が存在しない場合には、最適S-box決定手段は、こうして求めた、S-box候補とMDS行列の組合せの複雑度、S-box候補とその逆行列の組合せの複雑度から、ともに、その複雑度が大きな候補を選択することで、最適なS-boxとMDS行列の組合せを決定する(1010)。

【0078】この場合において、1006から1008の処理を省略し、1010において、MDS行列とS-boxの組合せの複雑度のみから最適なS-boxを決定する変形例が可能である。

【0079】図3では、S-boxは他の装置により決

定されたものを入力するとしたが、 $S-b \circ x$ についても、複数の候補のうち最適の組合せとなるものから選択する装置として実現する変形例も可能である。

【0080】図11は、図3の例に対して、 $S-b \circ x$ まで含めて最適な組合せを選択するように変形した装置の構成例を表す図である。図12は、その処理の流れを表す図である。図13は、さらに詳細にその処理を説明した図である。

【0081】本変形例の装置は、 $S-b \circ x$ 候補生成手段(1101)とMDS候補生成手段(1102)と組合せ評価値計算手段(1103)と最適 $S-b \circ x$ およびMDS行列決定手段(1104)とからなる。

【0082】 $S-b \circ x$ 候補生成手段は、 $S-b \circ x$ の候補を生成する(1201)。次に、MDS行列候補生成手段は、当該生成された $S-b \circ x$ 候補と組み合わせるMDS行列の候補を、逐次、生成する(1202)。次に、組合せ評価値計算手段は、当該生成された $S-b \circ x$ 候補と当該生成されたMDS行列候補の組合せの複雑度(評価値)を計算する(1203)。次に、今計算したMDS行列候補が最後の候補であるか否かを判定する(1204)。もし、まだ、新たな候補が存在する場合には、1202の処理に戻り、新たなMDS行列候補を生成する。こうして、逐次生成された、複数のMDS行列候補に対して同様の処理を繰り返し、その各々に対して組合せの複雑度を求める。もし、1204において新たなMDS行列候補が存在しないと判定した場合は、次に $S-b \circ x$ 候補として新たな候補が存在するか判定する。もし、また、新たな候補が存在する場合には、1201に戻り、新たな $S-b \circ x$ 候補に対して同様の処理を繰り返す。もし、1204において新たな $S-b \circ x$ 候補が存在しないと判定した場合には、最適 $S-b \circ x$ およびMDS行列決定手段は、これまでに求めたMDS候補と $S-b \circ x$ 候補に対する複雑度をもとに最適なMDS行列と $S-b \circ x$ の組み合わせを決定する(1206)。

【0083】より詳細に処理を説明する。まず、 $S-b \circ x$ 候補生成手段によって、 $S-b \circ x$ の候補の生成が行われる(1301)。組合せ評価値計算手段は、この生成された $S-b \circ x$ 候補における出力を入力で表した多項式を求める(1302)。次に、MDS行列候補生成手段は、MDS行列の行列要素の候補として取りうる値を生成する(1303)。組合せ評価値計算手段は、 $S-b \circ x$ 候補の出力に、この行列要素の候補を乗算した結果について、 $S-b \circ x$ 候補の入力による多項式を計算する(1304)。この多項式に基づき、 $S-b \circ x$ 候補とこの行列要素の候補の組合せに対する複雑度を計算する(1305)。複雑度としては、 $GF(2^n)$ の元とみなして、入力で表現した出力の多項式の項数を用いる。もちろん、項数を求める代わりに、多項式の次数によって複雑度を定義しても良い。また、別の、複雑

度の例としては、出力ビットを入力ビットの多項式で表現した場合の項数で定義しても良い。その際、項数は、すべての次数の項数を同じ重みで数えてもよいし、次数に応じて重み付きで数えても良い。次に、まだ別の行列要素の候補が存在するか否かを判定する(1306)。まだ、別の候補が存在する場合には、1303の処理にもどり新たな候補を生成して同様の処理を繰り返す。別の候補が存在しない場合には、行列要素の候補の中から必要な個数の候補を選択し、MDS行列の候補を生成する(1307)。

【0084】実際、この候補がMDS行列となっているか否かを判定する(1308)。この判定は、MDS行列の候補が、すべての小行列式が非零であることを確認することによって行われる。行列候補がMDS行列とならない場合には、1307の処理にもどり、次の行列候補を生成して同様の処理を繰り返す。行列候補がMDS行列となっている場合は、行列の複雑度の計算を行う(1309)。これは、1305において求めた $S-b \circ x$ 候補と行列要素の候補の組合せに対する複雑度を元に、行列候補に属する行列要素の候補に対する複雑度を足し合わせることで計算する。次に、逆行列を求める(1310)。

【0085】そして、逆行列に対しても1309と同様に行列の複雑度を求める(1311)。次に、 $S-b \circ x$ 候補としてこれが最後であるか否かを判定する(1312)。もし、まだ新たな $S-b \circ x$ 候補が存在する場合には、1301に戻り新たな $S-b \circ x$ 候補を生成して、同様の処理を繰り返す。最後の $S-b \circ x$ 候補の場合には、最適 $S-b \circ x$ 及びMDS行列決定手段は、 $S-b \circ x$ 候補とMDS行列候補の組合せのうち、 $S-b \circ x$ 候補とMDS行列の組合せの複雑度と、 $S-b \circ x$ と逆行列の組合せの複雑度のいずれもが大きな複雑度となるものを最適な $S-b \circ x$ とMDS行列の組合せと決定する(1313)。

(第2実施形態)

【0086】次に、図14は、以上に述べた $S-b \circ x$ とMDS行列の最適な組合せを与える装置によって決定された $S-b \circ x$ やMDS行列を採用する暗号化装置の構造を表す図である。1401は、暗号化装置のデータ攪拌を行う部分を表しており、平文を入力して暗号文を出力する。1401は、その構造の一部として、例えば、複数の $S-b \circ x$ によって構成される換字層1403と、例えば、MDS行列によって構成される拡散層1404を持つ。拡散層804は換字層803に直列に接続している。1402はデータ攪拌部のうち1403と1404以外の残りの暗号化処理部分である。1402の中にも1403と1404と同じ構造が含まれていても良い。

【0087】ここで、換字層1403と拡散層1404は、その一方もしくはその両方が、第1実施形態におい

て説明されたS-b o xまたはMDS行列またはその両方を決定する装置によって決定されたパラメータを持つ。これにより、1401のデータ攪拌文は、補間攻撃に対する安全性に優れたものであったり、アバランシュ性の良いものであったり、第1実施形態において選択した評価値の定義が意図していた望ましい性質に関して最適なS-b o xとMDS行列の組合せを与えるものとなっている。

【0088】このデータ攪拌部1401の動作について説明すると、平文が1401に入力されると、その入力には各種の変換を受けつつ、やがて、1402から換字層1403へと入力渡される。換字層1403は、複数のS-b o xで構成されており、各S-b o xは受け取った入力に対して換え字を行った結果を出力する。S-b o xの出力は、次の拡散層へと入力される。拡散層1404はMDS行列として表現され、拡散層1403からの入力に対して行列演算を施した結果を出力し、その出力を残りの暗号化処理部1402に返す。残りの暗号化処理部は、拡散層1404から受け取ったデータに対してさらなる変換を行い、最終的には暗号文として出力する。

【0089】ここでは、残りの暗号化部1402は、ひとつの部分からなる構造として表現されているが、換字層1403より前の部分と拡散層1404より後の部分の2つに分離した構造をしていても良い。また、その一方は、無くてもよい。

【0090】さらに、説明では換字層1403と拡散層1404は直結していたが、両者の間に例えば、拡大鍵加算のような別の処理が挟まっても良い。拡大鍵加算は、拡散層1404と順序を交換することで、線形変換によって得られる別の値の拡大鍵を1404の後に加算するのと同様であるからである。

【0091】なお、以上の実施形態の説明においては、換字層の後に拡散層が続く例によって最適な組合せを決定する方式を例にとりて説明を行ったが、拡散層の後に換字層が続く場合や、複数の換字層が続く場合、複数の拡散層が続く場合、換字層と拡散層が任意の順で任意の数ずつ交互に積み重なる場合、などにおいても、同様に、組合せの評価値を求めて最適化を行う変形例も可能である。

【0092】本発明の各実施形態は、装置による実施形態を述べたが、汎用のコンピュータ上で動作するソフトウェアプログラムとしても実現可能である。

【発明の効果】

【0093】以上説明したように本発明によれば、従来、S-b o xとMDS行列を構成要素に含む暗号化装置において、S-b o xとMDS行列が、それぞれ、独立な設計方針により最適な複雑さを実現しようとしているにもかかわらず、相互に効果を相殺するで、かえってより安全ではない暗号化装置となってしまう恐れがあっ

たが、MDS行列要素の各候補に対して、ある与えられたS-b o xに行列要素の乗算を行った結果の複雑さを評価し、この複雑さの評価結果に基づき、MDS行列を構成する行列要素候補の組合せに対する複雑さの評価を与え、また、このMDS行列に対する逆行列に対しても同様の複雑さの評価を与え、これらの行列に対する複雑さの評価結果に基づき、ある与えられたS-b o xと組合せにおいて、最適の複雑さを与えるMDS行列を決定することによって、互いの効果が相殺しない最適な組合せを決定することができるようになり、ひいては、そのように決定されたS-b o xやMDS行列を採用したより安全な暗号化装置を与えることができる。

【図面の簡単な説明】

【図1】本発明における与えられたS-b o xに対して最適な組合せのMDS行列を決定する装置の構成を表す図。

【図2】本発明における与えられたS-b o xに対して最適な組合せのMDS行列を決定する装置の処理を表す図。

【図3】本発明における与えられたS-b o xに対して最適な組合せのMDS行列を決定する装置の処理の詳細を表す図。

【図4】S-b o xと行列要素候補の組合せにおける複雑度を表す図。

【図5】S-b o xとMDS行列の組合せにおける複雑度を表す図。

【図6】本発明における与えられたMDS行列に対して最適な共通因子を決定する装置の構成を表す図。

【図7】本発明における与えられたMDS行列に対して最適な共通因子を決定する装置の処理を表す図。

【図8】本発明における与えられたMDS行列に対して最適な組合せのS-b o xを決定する装置の構成を表す図。

【図9】本発明における与えられたMDS行列に対して最適な組合せのS-b o xを決定する装置の処理の詳細を表す図。

【図10】本発明における与えられたMDS行列に対して最適な組合せのS-b o xを決定する装置の処理の詳細を表す図。

【図11】本発明における最適なS-b o xとMDS行列の組合せを決定する装置の構成を表す図。

【図12】本発明における最適なS-b o xとMDS行列の組合せを決定する装置の処理を表す図。

【図13】本発明における最適なS-b o xとMDS行列の組合せを決定する装置の処理の詳細を表す図。

【図14】本発明における最適なS-b o xまたはMDS行列またはその両方を用いた暗号化装置を表す図。

【符号の説明】

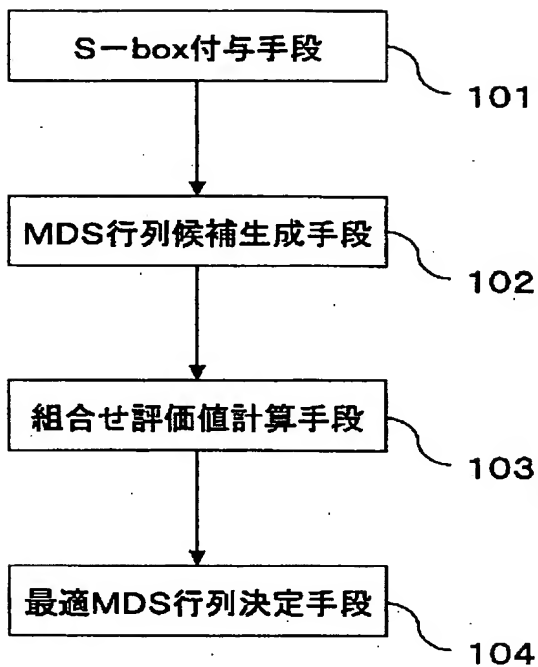
101 S-b o x付与手段

102 MDS行列候補生成手段

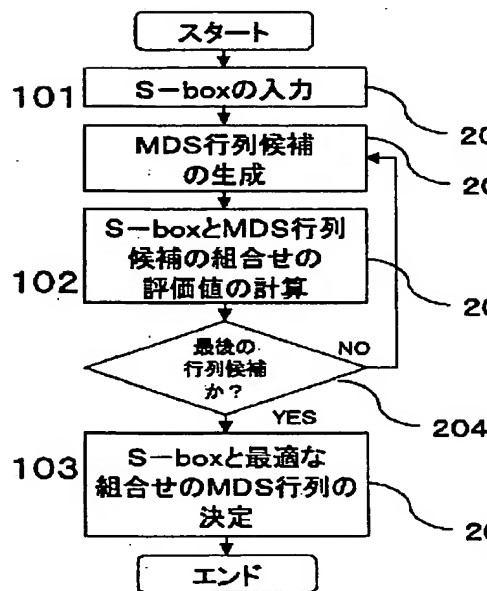
103 組合せ評価値計算手段
 104 最適MDS行列決定手段
 401 S-box
 402 行列要素候補
 501 S-box
 502 MDS行列
 601 MDS行列付与手段
 602 共通因子候補生成手段
 603 コスト評価値計算手段
 604 最適共通因子決定手段
 801 MDS行列付与手段

802 S-box候補生成手段
 803 組合せ評価値計算手段
 804 最適S-boxおよびMDS行列決定手段
 1101 S-box候補生成手段
 1102 MDS行列生成手段
 1103 組合せ評価値計算手段
 1104 最適S-boxおよびMDS行列決定手段
 1401 暗号化処理部 (データ攪拌部)
 1402 その他の暗号化処理部
 1403 S-box
 1404 MDS行列

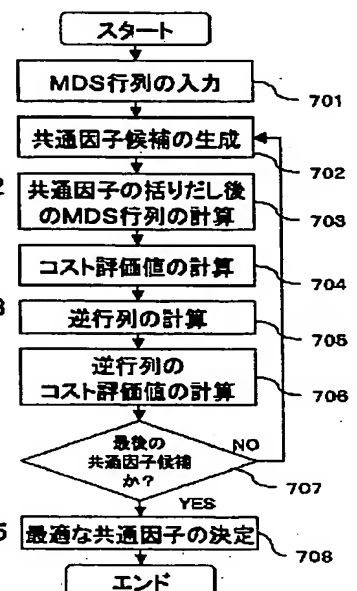
【図1】



【図2】

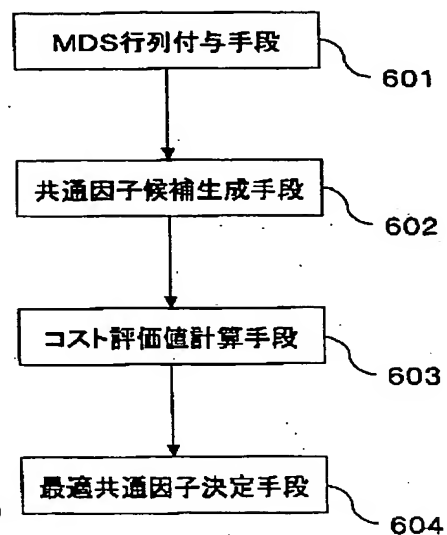
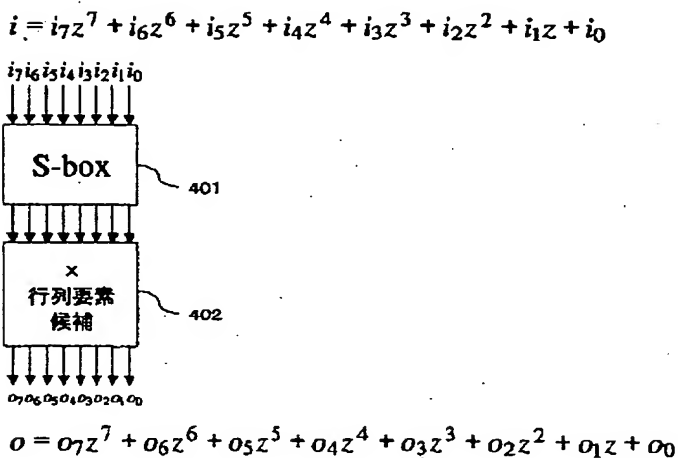


【図7】

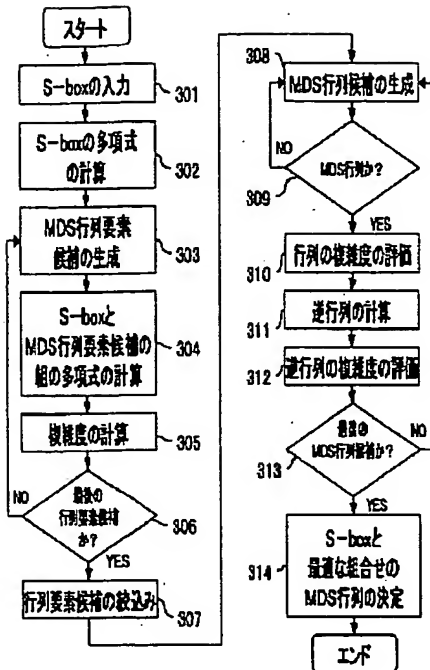


【図6】

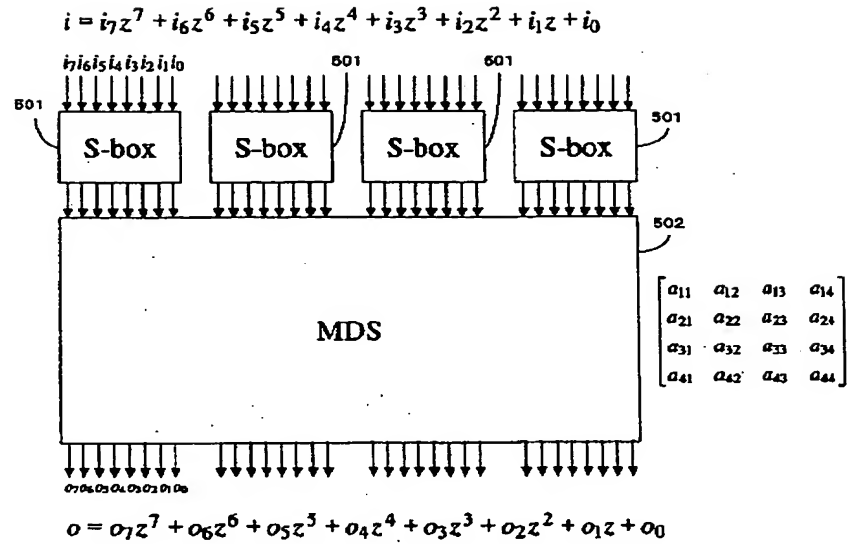
【図4】



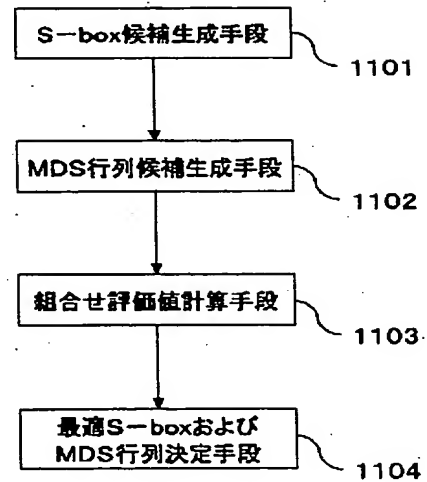
【図3】



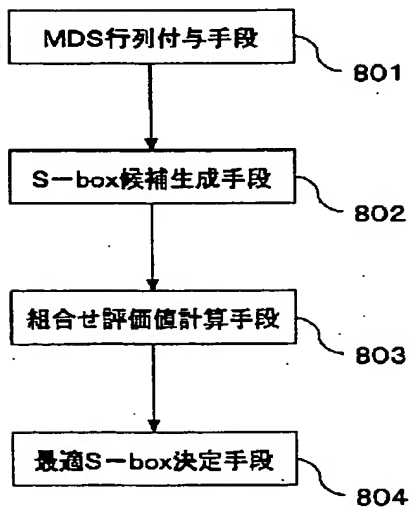
【図5】



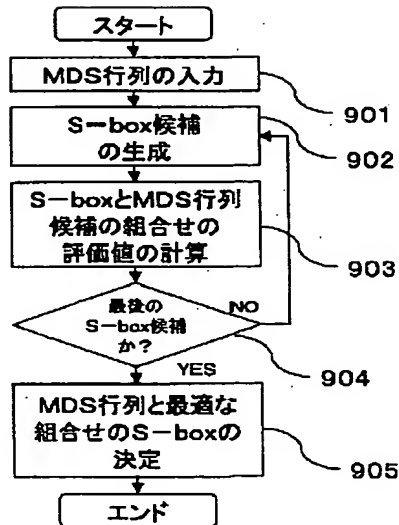
【図11】



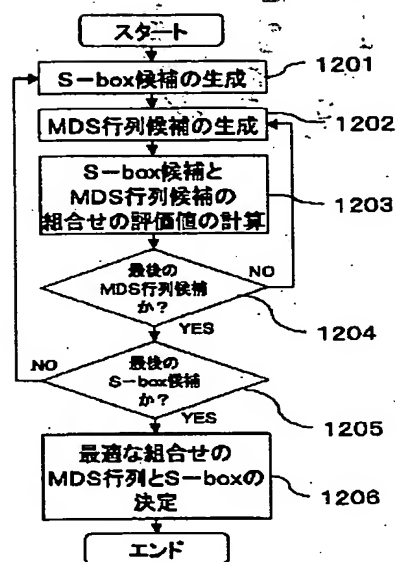
【図8】



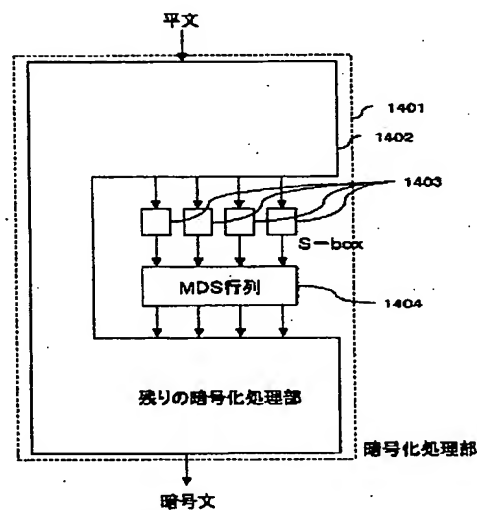
【図9】



【図.1-2】



【图 14】



(72)発明者 川村 信一
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内
Fターム(参考) 5J104 AA41 JA09 JA17 NA08 NA10